

# **Exhibit C**

# **Exhibit C.1**

*Homeland Security Investigations  
Office of the Executive Associate Director*


U.S. Department of Homeland Security  
500 12th Street, SW  
Washington, D.C. 20536



**U.S. Immigration  
and Customs  
Enforcement**

AUG 31 2017

MEMORANDUM FOR: Assistant Directors  
Deputy Assistant Directors  
Special Agents in Charge  
Attachés

FROM: ✓ Derek N. Benner   
Acting Executive Associate Director

SUBJECT: Use of Cell-Site Simulator Technology

Purpose:

Cell-site simulators are invaluable law enforcement tools that locate or identify mobile devices during active criminal investigations. They allow law enforcement to locate both subjects of an investigation and victims of ongoing criminal activity. U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) Special Agents (SAs), Technical Enforcement Officers (TEOs), and Task Force Officers (TFOs) may use cell-site simulators in accordance with the Department of Homeland Security (DHS) Policy Directive 047-02, "Department Policy Regarding the Use of Cell-Site Simulator Technology," dated October 19, 2015.

As with any law enforcement capability, HSI must use cell-site simulators in a manner that is consistent with the requirements and protections of the Constitution, including the Fourth Amendment and applicable statutory authorities, including the Pen Register Statute (Title 18, United States Code (U.S.C.), Section 3121 *et seq.*). Moreover, any information resulting from the use of cell-site simulators must be handled in a way that is consistent with applicable statutes, regulations, and policies that guide HSI data collection, retention, and disclosure.

By this memorandum, I am directing the immediate implementation of this HSI policy on the use of cell-site simulator technology. This policy provides guidance for the use of cell-site simulators by HSI SAs, TEOs, and TFOs. This policy applies solely to the use of cell-site simulator technology inside the United States, as well as inside its Commonwealths, Territories, and Possessions, in furtherance of criminal investigations.

SUBJECT: Use of Cell-Site Simulator Technology  
Page 2 of 7

Background:

HSI SAs, TEOs, and TFOs may use cell-site simulators to help locate cellular devices whose unique identifiers are already known to law enforcement, or to determine the unique identifiers of an unknown device by collecting limited signaling information from devices in the simulator user's vicinity.

Cell-site simulators, as governed by this policy, function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the cell-site device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the cellular device in the same way that they would with a networked tower.

A cell-site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular device. When used to identify an unknown device, the cell-site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device.

By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. Cell-site simulators provide only the relative signal strength and general direction of the subject cellular device; they do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. Cell-site simulators used by HSI SAs, TEOs, and TFOs must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes contents of any communication stored on the device itself; cell-site simulators do not remotely capture emails, text messages, contact lists, or images. Moreover, cell-site simulators used by HSI SAs, TEOs, and TFOs do not provide subscriber account information (for example, an account holder's name, address, or telephone number). Nothing in this policy prohibits the use of other appropriate legal authorities to acquire that information.

Management Controls and Accountability

The following management controls and approval processes will help ensure that only knowledgeable and accountable personnel will use the technology.

1. The HSI Assistant Director (AD), Information Management Directorate (IMD), will be responsible for the implementation of this policy and for ensuring compliance with its provisions within HSI. The AD, IMD, will also serve as the ICE executive level point of contact.
2. Prior to the court order application for the deployment of this technology, the use of a cell-site simulator must be approved by a first-level supervisor. Any exigent or

SUBJECT: Use of Cell-Site Simulator Technology  
Page 3 of 7

emergency use of a cell-site simulator must also be approved by an appropriate second-level supervisor prior to its use. If the circumstances permit, these approvals should be granted in writing (an email fulfills this requirement). When circumstances do not permit, approval should be documented in writing at the soonest practicable moment.

3. All users of cell-site simulators are required to attend training before using the equipment, which is required to include training on both privacy and civil liberties. The Unit Chief of the HSI Technical Operations Unit is responsible for the development and coordination of the initial and advanced training requirements for the use of cell-site simulators.

#### Legal Process and Court Orders

The use of cell-site simulators is permitted only as authorized by law and policy. While HSI SAs, TEOs, and TFOs have, in the past, appropriately obtained authorization to use a cell-site simulator by seeking an order pursuant to the Pen Register Statute, as a matter of policy, HSI SAs, TEOs, and TFOs must now obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or applicable state equivalent), except as provided below.

HSI SAs, TEOs, and TFOs will need to seek authority pursuant to Rule 41 *and* the Pen Register Statute, depending on the rules in their jurisdiction, prior to using a cell-site simulator. They must therefore consult with the Assistant United States Attorney (AUSA) or the appropriate state or local prosecutor, depending on the jurisdiction in which the cell-site simulator is being utilized, to either (1) obtain a warrant that contains all information required to be included in a pen register order pursuant to 18 U.S.C. § 3123 (or the state equivalent), or (2) seek a warrant and a pen register order concurrently. The search warrant affidavit must also reflect the information noted below under “Applications for Use of Cell Site Simulators.” In addition to consulting with the appropriate prosecuting attorney, HSI SAs, TEOs, and TFOs shall coordinate with their local Office of the Principal Legal Advisor (OPLA) prior to beginning the legal process or, in the case of exigent circumstances, as soon as practicable thereafter.

There are two circumstances in which this policy does not require a warrant prior to the use of a cell-site simulator.

1. *Exigent Circumstances under the Fourth Amendment*

Exigent circumstances can vitiate a Fourth Amendment warrant requirement, but cell-site simulators still require court approval – consistent with the circumstances delineated in the Pen Register Statute’s emergency provisions – in order to be lawfully deployed. An exigency that excuses the need to obtain a warrant may arise when the needs of law enforcement are so compelling that they render a warrantless search objectively reasonable. When an officer has the requisite probable cause, a variety of types of exigent circumstances may justify dispensing with a warrant. These include the need to protect human life or avert serious injury; the prevention of

SUBJECT: Use of Cell-Site Simulator Technology  
Page 4 of 7

the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice.

In this circumstance, the use of a cell-site simulator still must comply with the Pen Register Statute, 18 U.S.C. § 3121, *et seq.*, which ordinarily requires judicial authorization before use of the cell-site simulator, based on the government's certification that the information sought is relevant to an ongoing criminal investigation. In addition, in the subset of exigent situations where circumstances necessitate emergency pen register authority pursuant to 18 U.S.C. § 3125 (or the state equivalent), the emergency must be among those listed in Section 3125: immediate danger of death or serious bodily injury to any person; conspiratorial activities characteristic of organized crime; an immediate threat to a national security interest; or an ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030) that constitutes a crime punishable by a term of imprisonment greater than one year. Further, this policy requires that the case agent or operator first obtain the requisite supervisory approval to use a pen register before using a cell-site simulator.<sup>1</sup> In order to comply with the terms of this policy and with 18 U.S.C. § 3125, the case agent or operator must contact the duty AUSA in the local U.S. Attorney's Office, who will coordinate approval within the Department of Justice (DOJ).<sup>2</sup> Upon approval, the AUSA or the state or local prosecutor must also apply for a court order within 48 hours as required by 18 U.S.C. § 3125.<sup>3</sup> Under the provisions of the Pen Register Statute, use under emergency pen-trap authority must end when the information sought is obtained, an application for an order is denied, or 48 hours have passed, whichever comes first.

## 2. Training and Function Testing

All HSI SAs, TEOs, and TFOs who operate cell-site simulator equipment must have attended formal training provided by the equipment vendor and any other training determined necessary by the AD, IMD. These operators are required to take an annual refresher course on the requirements of this policy, including training on privacy and civil liberties, which will be furnished by the HSI Technical Operations Unit.

During practical training scenarios, HSI personnel are permitted to target specified government- or vendor-provided equipment intended for use in training purposes. Non-approved devices and civilian devices will not be used as targets during training scenarios.

As part of the pre-deployment of cell site simulator equipment, HSI operators should verify that the equipment is in proper working condition and confirm that the equipment has been cleared of all previous operational data, if it pertains to an unrelated mission, prior to deploying the equipment.

<sup>1</sup> (b)(7)(E)

<sup>2</sup> In non-federal cases, the case agent or operator must contact the prosecutor and any other applicable points of contact for the state or local jurisdiction.

<sup>3</sup> The knowing use of a pen register under emergency authorization without applying for a court order within 48 hours is a criminal violation of the Pen Register Statute, pursuant to 18 U.S.C. § 3125(c).



SUBJECT: Use of Cell-Site Simulator Technology  
Page 5 of 7

### Applications for Use of Cell-Site Simulators

In all circumstances, candor to the court is of paramount importance. When making any application to a court, HSI SAs, TEOs, and TFOs must disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. HSI SAs, TEOs, and TFOs must consult with the AUSA or appropriate prosecuting attorney in advance of using a cell-site simulator, and applications for the use of a cell-site simulator must include sufficient information to ensure that the courts are aware that the technology may be used.<sup>4</sup>

1. Regardless of the legal authority relied upon, at the time of making an application for use of a cell-site simulator, the application or supporting affidavit should describe in general terms the technique to be employed. The description should indicate that SAs, TEOs, or TFOs plan to send signals to the cellular device that will cause both the cellular device and non-target devices on the same provider network in close physical proximity to emit unique identifiers, which will be obtained by the technology. The description should also indicate that SAs, TEOs, and TFOs will use the information to determine the physical location of the target device or to determine the currently unknown identifiers of the target device. If SAs, TEOs, or TFOs will use the equipment to determine unique identifiers at multiple locations and/or multiple times at the same location, the application should indicate this also.
2. An application or supporting affidavit should inform the court that the target cellular device (e.g., cell phone) and other cellular devices in the area of influence of the cell-site simulator might experience a temporary disruption of service from the service provider. Generally, in a majority of cases, any disruptions are exceptionally minor in nature and virtually undetectable to end users. The application may also note, if accurate, that any potential service disruption would be temporary and all operations will be conducted to ensure the minimal amount of interference to non-target devices.<sup>5</sup>
3. An application for the use of a cell-site simulator should inform the court about how HSI intends to address deletion of data not associated with the target device. The application should also indicate that HSI will make no affirmative investigative use of any non-target data absent further order of the court, except to identify and distinguish the target device from other devices.

---

<sup>4</sup> Courts in certain jurisdictions may require additional technical information regarding the cell-site simulator's operation (e.g., tradecraft, capabilities, limitations, or specifications). Sample applications containing such technical information are available from the Computer Crime and Intellectual Property Section (CCIPS) of the DOJ's Criminal Division. To ensure that courts receive appropriate and accurate information regarding the technical information described above, prior to filing an application that deviates from the sample filings, SAs, TEOs, TFOs, or the prosecuting attorney must contact CCIPS, as well as consult with the local OPLA office for compliance with DHS policies.

<sup>5</sup> Despite any disruption in service, cell phones being disrupted will still be able to conduct emergency calls, i.e., 911.

SUBJECT: Use of Cell-Site Simulator Technology  
Page 6 of 7

#### Data Collection, Recordkeeping, and Disposal

HSI is committed to ensuring that law enforcement practices concerning the collection or retention<sup>6</sup> of data are lawful and respect the important privacy interests of individuals. As part of this commitment, HSI will operate in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personally identifiable information. As with data collected in the course of any investigation, these authorities apply to information collected through the use of a cell-site simulator. Consistent with applicable existing laws and requirements, including any duty to preserve exculpatory evidence,<sup>7</sup> HSI's use of cell-site simulators shall include the following practices:

1. Immediately following the completion of a mission, an operator of a cell-site simulator must delete all data.<sup>8</sup>
2. When the equipment is used to locate a target, data must be deleted as soon as the target is located.
3. When the equipment is used to identify a target, data must be deleted as soon as the target is identified, and no less than once every 30 days.
4. Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data.
5. If the deployment of the device results in the positive identification or location of a target person (or target telephone number), the said pertinent results will be documented in an ROI. The ROI will be stored in the relevant investigative case file and retained in accordance with the applicable Federal records schedule.

#### State and Local Partners

HSI often works closely with its state and local law enforcement partners and provides technological assistance under a variety of circumstances. In all cases, law enforcement authorities in the United States must conduct their missions lawfully and in a manner that respects the rights of the citizens they serve. This policy applies to all instances in which HSI uses cell-site simulators in support of other Federal agencies and/or state and local law enforcement agencies.

---

<sup>6</sup> In the context of this policy, the terms "collection" and "retention" are used to address only the unique technical process of identifying, dialing, routing, addressing, or signaling information, as described by 18 U.S.C. § 3127(3), emitted by cellular devices. "Collection" means the process by which unique identifier signals are obtained; "retention" refers to the period during which the dialing, routing, addressing, or signaling information is utilized to locate or identify a target device, continuing until the point at which such information is deleted.

<sup>7</sup> It is not likely, given the limited type of data cell-site simulators collect (as discussed above), that exculpatory evidence would be obtained by a cell-site simulator in the course of criminal law enforcement investigations. As in other circumstances, however, to the extent that investigators know or have reason to believe that information is exculpatory or impeaching, they have a duty to memorialize that information.

<sup>8</sup> A typical mission may last anywhere from less than one day up to several days.



SUBJECT: Use of Cell-Site Simulator Technology  
Page 7 of 7

#### Coordination and Ongoing Management

Each Special Agent in Charge office shall send monthly records to the Technical Operations Unit reflecting the total number of times a cell-site simulator is deployed, and by whom, in its area of responsibility; the number of deployments at the request of other agencies, including state or local law enforcement agencies; and the number of times the technology is deployed in exigent circumstances.<sup>9</sup> In these monthly records, confirmation that the equipment had been cleared of any previous operational data must also be included. The Technical Operations Unit will be responsible for monitoring and maintaining the monthly records.

#### Improper Use of Cell-Site Simulators

Accountability is an essential element in maintaining the integrity of HSI. Allegations of violations of any orders that implement this policy, as with other allegations of misconduct, will be referred to the Joint Intake Center and/or the ICE Office of Professional Responsibility.

#### No Private Right

This policy guidance is not intended to and does not create any right, benefit, trust or responsibility, whether substantive or procedural, enforceable at law or equity by a party against the United States, its departments, agencies, instrumentalities, entities, officers, employees, or agents, or any person, nor does it create any right of review in an administrative, judicial, or any other proceeding.

---

<sup>9</sup> Records reflecting the number of times the cell-site simulators were used may also be required for ongoing oversight by the DHS oversight offices.

# **Exhibit C.2**

SUBJECT: Use of Cell-Site Simulator Technology

Page 4 of 7

the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice.

In this circumstance, the use of a cell-site simulator still must comply with the Pen Register Statute, 18 U.S.C. § 3121, *et seq.*, which ordinarily requires judicial authorization before use of the cell-site simulator, based on the government's certification that the information sought is relevant to an ongoing criminal investigation. In addition, in the subset of exigent situations where circumstances necessitate emergency pen register authority pursuant to 18 U.S.C. § 3125 (or the state equivalent), the emergency must be among those listed in Section 3125: immediate danger of death or serious bodily injury to any person; conspiratorial activities characteristic of organized crime; an immediate threat to a national security interest; or an ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030) that constitutes a crime punishable by a term of imprisonment greater than one year. Further, this policy requires that the case agent or operator first obtain the requisite supervisory approval to use a pen register before using a cell-site simulator.<sup>1</sup> In order to comply with the terms of this policy and with 18 U.S.C. § 3125, the case agent or operator must contact the duty AUSA in the local U.S. Attorney's Office, who will coordinate approval within the Department of Justice (DOJ).<sup>2</sup> Upon approval, the AUSA or the state or local prosecutor must also apply for a court order within 48 hours as required by 18 U.S.C. § 3125.<sup>3</sup> Under the provisions of the Pen Register Statute, use under emergency pen-trap authority must end when the information sought is obtained, an application for an order is denied, or 48 hours have passed, whichever comes first.

## 2. Training and Function Testing

All HSI SAs, TEOs, and TFOs who operate cell-site simulator equipment must have attended formal training provided by the equipment vendor and any other training determined necessary by the AD, IMD. These operators are required to take an annual refresher course on the requirements of this policy, including training on privacy and civil liberties, which will be furnished by the HSI Technical Operations Unit.

During practical training scenarios, HSI personnel are permitted to target specified government- or vendor-provided equipment intended for use in training purposes. Non-approved devices and civilian devices will not be used as targets during training scenarios.

As part of the pre-deployment of cell site simulator equipment, HSI operators should verify that the equipment is in proper working condition and confirm that the equipment has been cleared of all previous operational data, if it pertains to an unrelated mission, prior to deploying the equipment.

---

<sup>1</sup> In accordance with the Technical Operations Handbook (HSI HB 14-01), dated July 21, 2014, or as updated.

<sup>2</sup> In non-federal cases, the case agent or operator must contact the prosecutor and any other applicable points of contact for the state or local jurisdiction.

<sup>3</sup> The knowing use of a pen register under emergency authorization without applying for a court order within 48 hours is a criminal violation of the Pen Register Statute, pursuant to 18 U.S.C. § 3125(c).